Module 2: Basic Switch and End Device Configuration

Instructor Materials

Introduction to Networks v7.0 (ITN)
2.1 - Cisco IOS Access
2.2 - IOS Navigation
2.3 - The Command Structure
2.4 - Basic Device Configuration
2.5 - Save Configurations
2.6 - Ports and Addresses
2.7 - Configure IP Addressing
2.8 - Verify Connectivity
Cisco IOS Access

Access Methods

- **Console** – A physical management port used to access a device in order to provide maintenance, such as performing the initial configurations.

- **Secure Shell (SSH)** – Establishes a secure remote CLI connection to a device, through a virtual interface, over a network. (Note: This is the recommended method for remotely connecting to a device.)

- **Telnet** – Establishes an insecure remote CLI connection to a device over the network. (Note: User authentication, passwords and commands are sent over the network in plaintext.)
IOS Navigation

Primary Command Modes

**User EXEC Mode:**
- Allows access to only a limited number of basic monitoring commands
- Identified by the CLI prompt that ends with the > symbol

**Privileged EXEC Mode:**
- Allows access to all commands and features
- Identified by the CLI prompt that ends with the # symbol
Global Configuration Mode:
- Used to access configuration options on the device

Line Configuration Mode:
- Used to configure console, SSH, Telnet or AUX access

Interface Configuration Mode:
- Used to configure a switch port or router interface
IOS Navigation

Navigation Between IOS Modes

- **Privileged EXEC Mode:**
  - To move from user EXEC mode to privilege EXEC mode, use the `enabled` command.

- **Global Configuration Mode:**
  - To move in and out of global configuration mode, use the `configure terminal` command. To return to privilege EXEC mode, use the `exit` command.

- **Line Configuration Mode:**
  - To move in and out of line configuration mode, use the `line` command followed by the management line type. To return to global configuration mode, use the `exit` command.

```plaintext
Switch> enable
Switch#

Switch(config)#
Switch(config)#exit
Switch#

Switch(config)#line console 0
Switch(config-line)#exit
Switch(config)#
```
Subconfiguration Modes:

• To move out of any subconfiguration mode to get back to global configuration mode, use the `exit` command. To return to privilege EXEC mode, use the `end` command or key combination `Ctrl +Z`.

• To move directly from one subconfiguration mode to another, type in the desired subconfiguration mode command. In the example, the command prompt changes from `(config-line)#` to `(config-if)#`.  

```sh
Switch(config)#line console 0
Switch(config-line)#end
Switch#

Switch(config-line)#interface FastEthernet 0/1
Switch(config-if)#
```
The Command Structure

Basic IOS Command Structure

- **Keyword** – This is a specific parameter defined in the operating system (in the figure, `ip protocols`).

- **Argument** - This is not predefined; it is a value or variable defined by the user (in the figure, `192.168.10.5`).
The Command Structure

IOS Help Features

The IOS has two forms of help available: context-sensitive help and command syntax check.

• Context-sensitive help enables you to quickly find answers to these questions:
  • Which commands are available in each command mode?
  • Which commands start with specific characters or group of characters?
  • Which arguments and keywords are available to particular commands?

• Command syntax check verifies that a valid command was entered by the user.
  • If the interpreter cannot understand the command being entered, it will provide feedback describing what is wrong with the command.

```
Router#ping ?
WORD Ping destination address or hostname
 ip IP echo
 ipv6 IPv6 echo
```

```
Switch#interface fastEthernet 0/1
^%
% Invalid input detected at '^' marker.
```
Basic Device Configuration

Device Names

• The first configuration command on any device should be to give it a unique hostname.

• By default, all devices are assigned a factory default name. For example, a Cisco IOS switch is "Switch."

• Guideline for naming devices:
  • Start with a letter
  • Contain no spaces
  • End with a letter or digit
  • Use only letters, digits, and dashes
  • Be less than 64 characters in length

Switch# configure terminal
Switch(config)# hostname Sw-Floor-1
Sw-Floor-1(config)#

Note: To return the switch to the default prompt, use the no hostname global config command.
Basic Device Configuration

Password Guidelines

• The use of weak or easily guessed passwords are a security concern.

• All networking devices should limit administrative access by securing privileged EXEC, user EXEC, and remote Telnet access with passwords. In addition, all passwords should be encrypted and legal notifications provided.

• Password Guidelines:
  • Use passwords that are more than eight characters in length.
  • Use a combination of upper and lowercase letters, numbers, special characters, and/or numeric sequences.
  • Avoid using the same password for all devices.
  • Do not use common words because they are easily guessed.

Note: Most of the labs in this course use simple passwords such as cisco or class. These passwords are considered weak and easily guessable and should be avoided in production environments.
Basic Device Configuration

Configure Passwords

Securing user EXEC mode access:

• First enter line console configuration mode using the `line console 0` command in global configuration mode.
• Next, specify the user EXEC mode password using the `password password` command.
• Finally, enable user EXEC access using the `login` command.

Securing privileged EXEC mode access:

• First enter global configuration mode.
• Next, use the `enable secret password` command.
Securing VTY line access:

- First enter line VTY configuration mode using the `line vty 0 15` command in global configuration mode.
- Next, specify the VTY password using the `password password` command.
- Finally, enable VTY access using the `login` command.

Note: VTY lines enable remote access using Telnet or SSH to the device. Many Cisco switches support up to 16 VTY lines that are numbered 0 to 15.
Basic Device Configuration
Encrypt Passwords

- The startup-config and running-config files display most passwords in plaintext.
- To encrypt all plaintext passwords, use the `service password-encryption` global config command.

Use the `show running-config` command to verify that the passwords on the device are now encrypted.

```plaintext
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# service password-encryption
Sw-Floor-1(config)# exit
Sw-Floor-1#
```
Basic Device Configuration

Banner Messages

- A banner message is important to warn unauthorized personnel from attempting to access the device.
- To create a banner message of the day on a network device, use the `banner motd # the message of the day #` global config command.

Note: The “#” in the command syntax is called the delimiting character. It is entered before and after the message.

Sw-Floor-1# configure terminal
Sw-Floor-1(config)# banner motd #Authorized Access Only!#

The banner will be displayed on attempts to access the device.

Press RETURN to get started.

Authorized Access Only!
User Access Verification
Password:
There are two system files that store the device configuration:

- **startup-config** - This is the saved configuration file that is stored in NVRAM. It contains all the commands that will be used by the device upon startup or reboot. Flash does not lose its contents when the device is powered off.

- **running-config** - This is stored in Random Access Memory (RAM). It reflects the current configuration. Modifying a running configuration affects the operation of a Cisco device immediately. RAM is volatile memory. It loses all of its content when the device is powered off or restarted.

To save changes made to the running configuration to the startup configuration file, use the `copy running-config startup-config` privileged EXEC mode command.

**Examples:**

```plaintext
Router#show startup-config
Using 624 bytes
!
version 15.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption

Router#show running-config
Building configuration...

Current configuration : 624 bytes
!
version 15.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
```
Save Configurations

Alter the Running Configurations

If changes made to the running config do not have the desired effect and the running-config has not yet been saved, you can restore the device to its previous configuration. To do this you can:

- Remove the changed commands individually.
- Reload the device using the `reload` command in privilege EXEC mode. *Note: This will cause the device to briefly go offline, leading to network downtime.*

If the undesired changes were saved to the startup-config, it may be necessary to clear all the configurations using the `erase startup-config` command in privilege EXEC mode.

- After erasing the startup-config, reload the device to clear the running-config file from RAM.

`Router# reload
Proceed with reload? [confirm]
Initializing Hardware ...
`

`Router# erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
$SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Router#`
Ports and Addresses

IP Addresses

• The use of IP addresses is the primary means of enabling devices to locate one another and establish end-to-end communication on the internet.

• The structure of an IPv4 address is called dotted decimal notation and is represented by four decimal numbers between 0 and 255.

• An IPv4 subnet mask is a 32-bit value that differentiates the network portion of the address from the host portion. Coupled with the IPv4 address, the subnet mask determines to which subnet the device is a member.

• The default gateway address is the IP address of the router that the host will use to access remote networks, including the internet.
Interfaces and Ports

- Network communications depend on end user device interfaces, networking device interfaces, and the cables that connect them.

- Types of network media include twisted-pair copper cables, fiber-optic cables, coaxial cables, or wireless.

- Different types of network media have different features and benefits. Some of the differences between various types of media include:
  - Distance the media can successfully carry a signal
  - Environment in which the media is to be installed
  - Amount of data and the speed at which it must be transmitted
  - Cost of the media and installation
Configure IP Addressing

Manual IP Address Configuration for End Devices

- End devices on the network need an IP address in order to communicate with other devices on the network.

- IPv4 address information can be entered into end devices manually, or automatically using Dynamic Host Configuration Protocol (DHCP).

- To manually configure an IPv4 address on a Windows PC, open the Control Panel > Network Sharing Center > Change adapter settings and choose the adapter. Next right-click and select Properties to display the Local Area Connection Properties.

- Next, click Properties to open the Internet Protocol Version 4 (TCP/IPv4) Properties window. Then configure the IPv4 address and subnet mask information, and default gateway.
Configure IP Addressing

Automatic IP Address Configuration for End Devices

- DHCP enables automatic IPv4 address configuration for every end device that is DHCP-enabled.

- End devices are typically by default using DHCP for automatic IPv4 address configuration.

- To configure DHCP on a Windows PC, open the Control Panel > Network Sharing Center > Change adapter settings and choose the adapter. Next right-click and select Properties to display the Local Area Connection Properties.

- Next, click Properties to open the Internet Protocol Version 4 (TCP/IPv4) Properties window, then select Obtain an IP address automatically and Obtain DNS server address automatically.

**Note:** IPv6 uses DHCPv6 and SLAAC (Stateless Address Autoconfiguration) for dynamic address allocation.
To access the switch remotely, an IP address and a subnet mask must be configured on the SVI.

To configure an SVI on a switch:

- Enter the `interface vlan 1` command in global configuration mode.
- Next assign an IPv4 address using the `ip address ip-address subnet-mask` command.
- Finally, enable the virtual interface using the `no shutdown` command.

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip address 192.168.1.20 255.255.255.0
Switch(config-if)# no shutdown
```
Verify Connectivity

Test the Interface Assignment

- Connect a console cable from the PC to the switch
- Use the terminal emulation program and accept the defaults to bring you to the command line
- Use enable to enter privileged EXEC mode
- Use the global configuration mode and the interface configuration mode to enter the no shutdown command